

ABSTRACT OF THE DISCLOSURE

An apparatus (10) for generating a sequence of blocks of randomly permuted multi-bit data elements includes an input register (12) that produces a repeating block of distinct input data elements from which output blocks of permuted data elements are generated. A permutation  
5 logic unit (14) forms an output data element from each input data element in accordance with random data stored in random code memories (16). The output data element produced by the permutation logic unit is supplied to an output register (18). The manner in which the random data is selected and applied by the permutation logic unit ensures that each of the data elements in the input block will be mapped into an output position in the output block.